

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400



PATENT APPLICATION

ATTORNEY DOCKET NO. 10016864-1

*AK*  
*JPW*

IN THE  
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard L. SCHERTZ et al.

Confirmation No.: 3588

Application No.: 10/002,072

Examiner: Gelagay, Shewaye

Filing Date: October 31, 2001

Group Art Unit: 2133

Title: SYSTEM AND METHOD OF AN OS-INTEGRATED INTRUSION DETECTION AND ANTI-VIRUS SYSTEM

Mail Stop Appeal Brief-Patents  
Commissioner For Patents  
PO Box 1450  
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on November 15, 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month  
\$120

☐ 2nd Month  
\$450

☐ 3rd Month  
\$1020

☐ 4th Month  
\$1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:  
Commissioner for Patents, Alexandria, VA 22313-1450  
Date of Deposit: January 11, 2006

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Cindy C. Dioso

Signature: Cindy C. Dioso

Respectfully submitted,

Richard L. SCHERTZ et al.

By: James L. Baudino

James L. Baudino

Attorney/Agent for Applicant(s)

Reg No. : 43,486

Date : January 11, 2006

Telephone : (214) 855-7544



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**APPEAL FROM THE EXAMINER TO THE BOARD  
OF PATENT APPEALS AND INTERFERENCES**

In re Application of: Richard L. SCHERTZ et al.  
Serial No.: 10/002,072  
Filing Date: 10/31/2001  
Group Art Unit: 2133  
Examiner: Gelagay, Shewaye  
Title: SYSTEM AND METHOD OF AN OS-INTEGRATED  
INTRUSION DETECTION AND ANTI-VIRUS SYSTEM  
Docket No.: 10016864-1

**MAIL STOP: APPEAL BRIEF PATENTS**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Dear Sir:

**APPEAL BRIEF**

Applicants has appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed September 19, 2005, finally rejecting Claims 1-29. Applicants filed a Notice of Appeal on November 15, 2005. Applicants respectfully submits herewith this Appeal Brief with authorization to charge the statutory fee of \$500.00.

01/18/2006 BABRAHA1 00000085 082025 10002072

01 FC:1402 500.00 DA

### **REAL PARTY IN INTEREST**

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on March 13, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012736, Frame 0255. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2003 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492.

### **RELATED APPEALS AND INTERFERENCES**

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

### **STATUS OF CLAIMS**

Claims 1-29 stand rejected pursuant to a Final Office Action mailed September 19, 2005. Claims 1-29 are presented for appeal.

### **STATUS OF AMENDMENTS**

No amendment has been filed subsequent to the mailing of the Final Office Action.

### **SUMMARY OF CLAIMED SUBJECT MATTER**

Embodiments of the present invention as defined by independent Claim 1 are directed toward a computer comprising an operating system (12) controlling a computer resource (18, 20, 22, 24, 26, 28, 30) and an intrusion detection system (14) integrated with the operating system (12) and operable to monitor the computer resources (18, 20, 22, 24, 26, 28, 30) to detect and prevent intrusion attempts. (at least at page 5, lines 21-32; page 6, lines 1-9; page 7, lines 30-32; page 8, lines 1-13 and 21-32; page 9, lines 7-32; page 10, lines 1-32; page 11, lines 9-28; and figures 1-4).

Embodiments of the present invention as defined by independent Claim 15 are directed toward a method comprising executing an OS (12)-integrated intrusion detection system (14) and monitoring at least one computer resource (18, 20, 22, 24, 26, 28, 30) to detect and prevent intrusion attempts. (at least at page 5, lines 21-32; page 6, lines 1-9; page 7, lines 30-32; page 8, lines 1-13 and 21-32; page 9, lines 7-32; page 10, lines 1-32; page 11, lines 9-28; and figures 1-4).

Embodiments of the present invention as defined by independent Claim 22 are directed toward a method comprising executing an OS (12)-integrated anti-virus system (16) and monitoring at least one computer resource (18, 20, 22, 24, 26, 28, 30) to detect the presence of at least one virus. (at least at page 5, lines 21-32; page 6, lines 1-9; page 7, lines 30-32; page 8, lines 1-13 and 21-32; page 9, lines 7-32; page 10, lines 1-32; page 11, lines 9-32; page 12, lines 1-13; and figures 1-5).

#### **GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

1. Claims 22-29 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,856,481 issued to Walsh (hereinafter "*Walsh*").
2. Claims 1-3 and 15-17 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,405,318 issued to Rowland (hereinafter "*Rowland*").
3. Claims 4, 5 and 10-14 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Rowland* in view of *Walsh*.
4. Claims 6-9 and 18-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Rowland* in view of U.S. Patent No. 6,405,318 issued to Holland, III et al. (hereinafter "*Holland*").

## ARGUMENT

### A. Standard

#### 1. 35 U.S.C. § 102

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, “[t]he identical invention must be shown in as complete detail as is contained in the . . . claims” and “[t]he elements must be arranged as required by the claim.” *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

#### 2. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant’s disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another

reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

B. Argument

1. First Ground of Rejection (Claims 22-29)

Claims 22-29 are rejected under 35 U.S.C. §102(b) as being anticipated by *Walsh*. Of the rejected claims, Claim 22 is independent. Applicants respectfully submit that independent Claim 22 is patentable over the *Walsh* reference and, therefore, Claim 22, and Claims 23-29 that depend therefrom, are allowable.

Embodiments of the present invention generally involve an intrusion detection system (14) and/or anti-virus system (16) integrated into an operating system (12) (at least at page 5, lines 21-32; page 6, lines 1-12; and figures 1 and 2). For example, in at least one embodiment of the present invention, the intrusion detection system (14) and/or anti-virus system (16) is integrated between predetermined layers of a layered protocol (100) (at least at page 9, lines 7-9; and figure 3). In such an embodiment, a first interface or access point of the OS (12)-integrated intrusion detection (14) and/or anti-virus (16) system comprises an integration I layer (105) that can filter raw network frames to protect the Internet protocol (IP) stack (106) disposed above it in the network layered architecture (at least at page 9, lines 16-29; and figure 3). A second interface or access point of the OS (12)-integrated intrusion detection (14) and/or anti-virus (16) system comprises an integration II layer (108) disposed between a network layer (106) and a transport layer (110) of the IP stack (100) to indicate that the integrated intrusion detection (14) and anti-virus (16) systems are able to access the data, session and control information that pass between these two protocol layers (106, 110) (at least at page 9, lines 30-32; page 10, lines 1-6; and figure 3). Disposed above transport layer (110) and below application layer (114) of the IP stack (100) is an integration III layer (112) to enable access to the data, session and control information that pass between transport layer (110) and application layer (114) (at least at page 10, lines 6-31; and figure 3). Accordingly, independent Claim 22 recites “executing an OS-integrated anti-virus

system” and “monitoring at least one computer resource to detect the presence of at least one virus.”

In the Final Office Action, the Examiner refers to column 2, lines 63-64, of *Walsh* as disclosing an “OS-integrated anti-virus system” as recited by independent Claim 22 (Final Office Action, page 4). Applicants respectfully disagree. Column 2, lines 63-64, of *Walsh* recites the following:

The present invention addresses the above needs by providing a system for protecting a computer from infection by a virus that attacks data files of an executable program.

Applicants respectfully submit that the portion of *Walsh* referenced by the Examiner fails to rise to the level required to support a rejection under 35 U.S.C. § 102. For example, the Examiner does not explicitly identify, either in the above-referenced portion of *Walsh* or elsewhere in *Walsh*, an anti-virus system integrated into an operating system. Applicants respectfully submit that such disclosure is apparently absent from *Walsh* and, accordingly, for at least this reason, *Walsh* does not anticipate independent Claim 22.

Further, *Walsh* appears to disclose an operating system 35 and an application program 36, such as Microsoft’s “WORD” program, and that the application program includes a virus check routine 36a as an internal component of the executable program (*Walsh*, column 8, lines 35-40). *Walsh* recites:

In one exemplary embodiment, the invention is incorporated into a word processing application program entitled “WORD FOR WINDOWS 95,” marketed by Microsoft Corporation of Redmond, Wash. Briefly described . . . virus protection is implemented as a routine or component internal to the “WORD” program. This allows the protection routine to readily recognize both internal and external file open events for a document that may contain a virus. Because the protection routine is implemented as an integral component of the “WORD” program, virus protection also can be offered for the

opening of a document residing on either a local machine or on a remote server.

(*Walsh*, column 7, lines 25-40). Thus, *Walsh* does not appear to disclose or even suggest an anti-virus system integrated into an operating system. To the contrary, *Walsh* appears to disclose a virus protection routine implemented in an application program. Accordingly, for at least these reasons, Applicants respectfully submit that independent Claim 22 is clearly patentable over *Walsh*. Therefore, Claim 22, and Claims 23-29 that depend therefrom, are in condition for allowance.

## 2. Second Ground of Rejection (Claims 1-3 and 15-17)

Claims 1-3, 15-17 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,405,318 issued to Rowland (hereinafter "*Rowland*"). Of the rejected claims, Claims 1 and 15 are independent. Applicants respectfully submit that independent Claims 1 and 15 are patentable over *Rowland* and, therefore, Claims 2, 3, 16 and 17 that depend respectively therefrom are also patentable.

Embodiments of the present invention generally involve an intrusion detection system (14) and/or anti-virus system (16) integrated into an operating system (12) (at least at page 5, lines 21-32; page 6, lines 1-12; and figures 1 and 2). For example, in at least one embodiment of the present invention, the intrusion detection system (14) and/or anti-virus system (16) is integrated between predetermined layers of a layered protocol (100) (at least at page 9, lines 7-9; and figure 3). In such an embodiment, a first interface or access point of the OS (12)-integrated intrusion detection (14) and/or anti-virus (16) system comprises an integration I layer (105) that can filter raw network frames to protect the Internet protocol (IP) stack (106) disposed above it in the network layered architecture (at least at page 9, lines 16-29; and figure 3). A second interface or access point of the OS (12)-integrated intrusion detection (14) and/or anti-virus (16) system comprises an integration II layer (108) disposed between a network layer (106) and a transport layer (110) of the IP stack (100) to indicate that the integrated intrusion detection (14) and anti-virus (16) systems are able to access the data, session and control



information that pass between these two protocol layers (106, 110) (at least at page 9, lines 30-32; page 10, lines 1-6; and figure 3). Disposed above transport layer (110) and below application layer (114) of the IP stack (100) is an integration III layer (112) to enable access to the data, session and control information that pass between transport layer (110) and application layer (114) (at least at page 10, lines 6-31; and figure 3). Accordingly, for example, independent Claim 1 recites “an operating system controlling a computer resource” and “an intrusion detection system integrated with the operating system and operable to monitor the computer resource to detect and prevent intrusion attempts.”

In the Final Office Action, the Examiner generally refers to column 2, lines 41-58 and 65-67, and column 3, lines 44-47, of *Rowland* as disclosing the limitations of independent Claim 1 (Final Office Action, page 6). Applicants respectfully disagree. The portions of *Rowland* referred to by the Examiner appear to be directed toward a system that builds user profile data (known as a signature) for each user (or alternately, a class of users) that can be used to determine normal actions for each user by comparing a user's past behavior with a user's current behavior (*Rowland*, column 2, lines 40-50). *Rowland* also appears to disclose that the *Rowland* system provides real-time monitoring of log audit files, port scan detection capability and session monitoring (e.g., the log audit function continuously monitors system log files for anomalous activity which can include known suspicious activity and unknown system anomalies) (*Rowland*, column 2, lines 65-67, column 3, lines 40-47). *Rowland* does not appear to disclose or even suggest, in the portions referred to by the Examiner or elsewhere in *Rowland*, an intrusion detection system integrated with an operating system as recited by Claim 1. Therefore, for at least this reason, Applicants respectfully submit that *Rowland* does not anticipate Claim 1.

In the Final Office Action, the Examiner also refers to column 4, lines 35-38, of *Rowland* as disclosing an intrusion detection system integrated with an operating system (Final Office Action, page 3). Applicants respectfully disagree. *Rowland* appears to disclose that particular files that are monitored for anomaly detection may be event logs

for a Windows NT® operating system (*Rowland*, column 4, lines 35-38). Applicants respectfully submit that monitoring the event logs of an operating system is not equivalent to an intrusion detection system integrated with or forming part of an operating system as generally recited by Claim 1. Accordingly, for at least this reason also, Applicants respectfully submit that *Rowland* does not anticipate independent Claim 1.

Independent Claim 15 recites “executing an OS-integrated intrusion detection system” and “monitoring at least one computer resource to detect and prevent intrusion attempts” (emphasis added). At least for the reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that *Rowland* also does not anticipate independent Claim 15.

Claims 2, 3, 16 and 17 depend respectively from independent Claims 1 and 15. At least for the reasons discussed above, Claims 1 and 15 are in condition for allowance. Therefore, Claims 2, 3, 16 and 17 that depend respectively therefrom are also allowable. Accordingly, Applicants respectfully submit that independent Claims 1 and 15 are clearly patentable over *Rowland* and, therefore, Claims 1 and 15, and Claims 2, 3, 16 and 17 that depend respectively therefrom, are in condition for allowance.

3. Third Ground of Rejection (Claims 4, 5 and 10-14)

Claims 4, 5 and 10-14 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Rowland* in view of *Walsh*. Claims 4, 5 and 10-14 depend from independent Claim 1. At least for the reasons discussed above, Claim 1 is in condition for allowance. Therefore, Claims 4, 5 and 10-14 that depend therefrom are also in condition for allowance. Moreover, *Walsh* does not appear to remedy, nor did the Examiner rely on *Walsh* to remedy, at least the deficiencies of *Rowland* indicated above. Accordingly, Applicants respectfully submit that at least for these reasons, Claims 4, 5 and 10-14 are in condition for allowance.

4. Fourth Ground of Rejection (Claims 6-9 and 18-21)

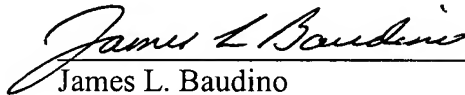
Claims 6-9 and 18-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Rowland* in view of *Holland*. Claims 6-9 and 18-21 depend respectively from independent Claims 1 and 15. At least for the reasons discussed above, Claims 1 and 15 are in condition for allowance. Therefore, Claims 6-9 and 18-21 that depend respectively therefrom are also in condition for allowance. Moreover, *Holland* does not appear to remedy, nor did the Examiner rely on *Holland* to remedy, at least the deficiencies of *Rowland* indicated above. Accordingly, Applicants respectfully submit that at least for these reasons, Claims 6-9 and 18-21 are in condition for allowance.

**CONCLUSION**

Applicants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicants respectfully request the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of \$500.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

  
James L. Baudino  
Registration No. 43,486

Date: January 11, 2006

Correspondence To:

L. Joy Griebenow  
Hewlett-Packard Company  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400  
Tel. (970) 898-3884

## **CLAIMS APPENDIX**

1. A computer comprising:  
an operating system controlling a computer resource; and  
an intrusion detection system integrated with the operating system and operable to monitor the computer resources to detect and prevent intrusion attempts.
2. The computer, as set forth in claim 1, wherein the computer resource is selected from the group consisting of data storage system, input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices.
3. The computer, as set forth in claim 1, wherein the computer resource comprises an application program execution environment and a networking system under the control of the operating system and monitored by the intrusion detection system to detect, prevent and report intrusion attempts.
4. The computer, as set forth in claim 1, further comprising an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect the presence of at least one virus.
5. The computer, as set forth in claim 1, further comprising an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus.
6. The computer, as set forth in claim 2, wherein intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames.

7. The computer, as set forth in claim 2, wherein the intrusion detection system is integrated with a networking stack of the networking system above the network layer operable to access reassembled fragments.

8. The computer, as set forth in claim 2, wherein the intrusion detection system is integrated with a networking protocol stack of the networking system above the transport layer.

9. The computer, as set forth in claim 2, wherein the intrusion detection system is integrated with a networking stack of the networking system between the network layer and the transport layer and between the transport layer and the application layer.

10. The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to prevent reassembly of a virus.

11. The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to recognize a virus.

12. The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to prevent storage of a virus.

13. The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to prevent transmission of a virus.

14. The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to prevent execution of a virus.

15. A method comprising:  
executing an OS-integrated intrusion detection system; and  
monitoring at least one computer resource to detect and prevent intrusion attempts.

16. The method, as set forth in claim 15, wherein monitoring at least one computer resource comprises monitoring at least one computer resource selected from the group consisting of a data storage system, an input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices.

17. The method, as set forth in claim 15, wherein monitoring at least one computer resource comprises reporting intrusion attempts.

18. The method, as set forth in claim 16, further comprising integrating the intrusion detection system with a networking system above the link layer operable to access raw network frames.

19. The method, as set forth in claim 15, further comprising integrating the intrusion detection system with a networking stack of the networking system above the network layer operable to access reassembled fragments.

20. The method, as set forth in claim 15, further comprising integrating the intrusion detection system with a networking protocol stack of the networking system above the transport layer.

21. The method, as set forth in claim 15, further comprising integrating the intrusion detection system with a networking stack of the networking system between the network layer and the transport layer, and between the transport layer and the application layer.

22. A method comprising:  
executing an OS-integrated anti-virus system; and  
monitoring at least one computer resource to detect the presence of at least one virus.

23. The method, as set forth in claim 22, wherein monitoring at least one computer resource comprises monitoring at least one computer resource selected from the group consisting of a data storage system, an input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices.

24. The method, as set forth in claim 22, wherein monitoring at least one computer resource comprises reporting the presence of at least one virus.

25. The method, as set forth in claim 22, wherein the step of monitoring comprises detecting the reassembly of a virus.

26. The method, as set forth in claim 22, wherein the step of monitoring comprises recognizing a virus.

27. The method, as set forth in claim 22, wherein the step of monitoring comprises preventing the storage of a virus.

28. The method, as set forth in claim 22, wherein the step of monitoring comprises preventing the transmission of a virus.

29. The method, as set forth in claim 22, wherein the step of monitoring comprises preventing the execution of a virus.



**EVIDENCE APPENDIX**

None

**RELATED PROCEEDINGS APPENDIX**

None